Set Task Electronic Template – Unit 11

Task A - Activity 2 Template: Cyber security plan for the networked system

Use the section headings below for each protection measure.
1) Threat(s) addressed by the protection measure
2) Details of action(s) to be taken
3) Reasons for the actions
4) Overview of constraints – technical and financial
5) Overview of legal responsibilities
6) Overview of usability of the system
7) Outline cost-benefit
8) Test plan

Protection measure 1.

Threats addressed – 5. Network access by guest and staff mobile devices could be an attack vector due to misconfigured SSID or encryption on Wi-Fi. Size of loss. Major.

Actions to be taken:
Ensure that Staff WAP is configured with WAP2 and has a strong password.
Additionally use a Mac address in order to white list staff on WAP.
For both staff and guest WAP enter correct SSID and key.

Reasons for actions:
The separate guest WAP should be configured so that access to the access to the WAP only allows for access to a restricted area of the BCTAA network, such as the internet.
By integrating a strong password on the Staff WAP it will increase the difficulty of attackers being able to gain unauthorised network access.
The use of a Mac access list would only for only pre-approved devices to connect to the Staff network which increases security and limits the number of devices able to connect.
A misconfigured SSID could result in guests attempting to connect to the wrong network, and potentially raising a security alert.
Also a misconfigured WAP2 and key could restrict the functionality of the network and leave points of weakness for attackers to exploit.

Constraints:
Technical: MAC white list. Medium. The list would be simple to set up but would have to be propagated to all staff WAPs. There may be a physical limit however on the on the size of the list the staff WAP will allow therefore there is a possibility of not enough space for all staff devices.
Financial: minimal. The staff WAP will most likely already include a MAC list capability therefore the financial constraint should be minimalistic.
Legal responsibilities:
None as long as confidential data is protected by other means such as encryption.
Usability: medium if MAC lists are included, however the enforcement of strong passwords may cause some logon errors such as locked accounts.

Cost – benefit. The possibility of a major system intrusion heavily outweighs the small cost required to implement the protection plan. The use a MAC lists is very desirable however it should be measured against the number of staff devices which require access to the network and the frequency at which they may change.

Test plan

Test No	Test description	Expected outcome	Possible further action following test
1	Select guest SSID, Logon to guest WAP and attempt to Access the BCTAA network.	Only authorised areas of the network will be available.	
2	Attempt to logon to staff WAP.	Logon screen requesting password should be displayed. Logon succeeds with correct password.	Repeat the test with each staff WAP to ensure that WAP2 and SSID has been configured correctly for each.
3.	When MAC list is used, attempt staff logon to staff WAP, with listed and unlisted devices.	Only listed devices will log on.	Repeat the test with each staff WAP to ensure the list has been properly integrated.

Protection measure 2.

Threats addressed – 2, 3, 7 Attack via electronic door control system, misconfigured firewall, size of loss. Major.

Actions to be taken:
Install active firewall if not already installed in the routers.
Configure internet firewall to allow access via ports required by the electronic door control system chosen. If possible change the ports from the default ones.
Network address translation to forward the electronic door control to the correct electronic door control system server.
Configure electronic door control system server.
For the WI-FI router, open ports 80, 443 and 993 only.

Reasons for actions:
Attacks on commonly use ports are frequent and automated therefore it is important to install a firewall in order to block and ignore pings unless the relevant port has been opened. Open ports for known software invites further, more targeted attacks. Changing the port number will resist automated attacks as the attack will be trying to compromise a software normally found using the new port.
For the WI-FI router ports 80, 443 and 993 allow http, https and email functions.

Constraints:
Technical: Minimal. Setup and configuration of firewalls are simple and walk through are freely available.
Financial: Minimal. A commercial quality router will almost always include a firewall
Legal responsibilities: None as long as the data is protected by other means such as encryption.
Usability: Minimal, as the installation of the firewall should only block malicious attacks.

Cost – benefit. The possibility of a major system intrusion is too dangerous in comparison to spending small amounts on correct security. It is vital that the measure is implemented.

Test No	Test description	Expected outcome	Possible further action following test
4	Use port scanner on firewalls.	Shows open ports.	Check use of all open ports, close any that are not required.
5	Perform external log in to server using correct and default ports.	Default ports should fail, correct ports should give access to server.	Reconfigure software and ports as required.
6	Attempt to access services other than browsing and email on the Wi-Fi system.	Other services should fail to connect.	Recheck software and ports as required.

Protection measure 3.

Threats addressed – 10. Unauthorised use of RJ45 ports. Size of loss. Medium.

Actions to be taken:
Fit a faceplate or port blocker to each port.

Reasons for actions:
Access to an RJ45 port could allow a device to be connected to the network, either active, trying to access files and trying to capture network traffic. Ports are also physically vulnerable and could be damaged, covers would help protect against physical damage.

Constraints:
Technical: Minimal. Port blockers and lockable faceplates are available for purchase. No expertise are required to fit a port blocker, lockable faceplates can be installed easily as opened ones.
Financial: Minimal. Port blockers and lockable faceplates are relatively cheap. They will most likely pay for themselves by reducing the the requirement to replace damaged ports.
Legal responsibilities: None as long as data is protected by other means such as encryption
Usability: Minimal. Once installed, staff who need to move RJ45 cables would need to use a key.

Cost – benefit. Overall, the cost of replacing ports is probably greater than the cost of protecting them. The extra security is a bonus. The protection measure needs to be implemented.

Test No	Test description	Expected outcome	Possible further action following test
7	Pre installation, attempt to tamper with a blocked port.	The block should be tamper proof to the extent threat removal of the block should render the port useless.	If the port still works, consider using a different blocking method.

Protection measure 4

Threats addressed – 1. Misconfigured NAT

Actions to be taken:
Turn on NAT, configure for Guest Wi-Fi and devices

Reasons for actions:
Lack of NAT will prevent use of Guest WI-FI and mobile devices. Misconfigured NAT could link external devices to parts of the system which cannot be expose to the internet.

Constraints:
Technical: Minimal. Setup and configuration tasks are simple and walk through are freely available.
Financial: Minimal. NAT software is built into most modern routers.
Legal responsibilities: None as long as the data is protected by other means such as encryption.
Usability: Minimal, Once installed staff who access the network from outside are likely to do so via vpn software which handles the connection process for them.

Cost – benefit. A small one time cost to set up the NAT system is easily balanced by the practical advantages of having a awfully working network for guest Wi-Fi and mobile devices.

Test No	Test description	Expected outcome	Possible further action following test
8	Attempt login to external guest WI-FI	Access should be granted to guest network.	If access is denied or connects to the wrong device, reconfigure and retry.

Protection measure 5

Threats addressed - 8. Admin server visible to WI-FI network.

Actions to be taken:
Apply net config hidden “yes” to the server

Reasons for actions:
Guests often float around on a network to what they can get access to. If the network does not appear on the guests WI_FI networks list it is less to be interfered with.

Constraints:
Technical: Minimal. Net config tasks are simple and walk through are freely available.
Financial: Minimal. Net config is part of the operating system.
Legal responsibilities: None as long as the data is protected by other means such as encryption.
Usability: Minimal, Users, such as staff who need to access the server can still do so however they will have to know the IP address.

Cost – benefit. A cost free option which will easy to carry out and will minimise the interference f the network is huge positive balance on the scales.

Test No	Test description	Expected outcome	Possible further action following test
9	Hide the server, reboot and then attempt to find it with discovery tools.	The server should not appear on the network list	If the server appears, rehide, reboot then repeat the test.

Protection measure 6

Threats addressed - 9. WI_FI must not connect to IOT devices.

Actions to be taken:
Use DHCP server to configure IP addresses, scopes and reservations. Set devices to obtain an address via DHCP.

Reasons for actions:
DHCP can be used to split the network into sectors which do not talk to each other unless they have permission and have been set up for that purpose. IoT devices could be given static addresses, so they don't chance after they reset. The addresses can be on a different sub net to all of the Wi-Fi addresses so that Wi-Fi devices cannot see or connect to IoT of devices.

Constraints:
Technical: Minimal. DHCP config tasks are simple and walk through are freely available.
Financial: Minimal. DHCP is part of the server operating system.
Legal responsibilities: None as long as the data is protected by other means such as encryption.
Usability: Minimal, correct addressing should be transparent to users, who will normally use share names or device icons to make connections.

Cost – benefit. Another cost free option which will easy to carry out and will minimise the interference f the network is huge positive balance on the scales.

Test No	Test description	Expected outcome	Possible further action following test
10.	Log on to WI-FI and attempt to locate a known Iot device with net discovery tools	The device should not appear on the network list	If the device appears check and amend DHCP settings and repeat the test.

Protection measure 7

Threats addressed – 11 . Attack via Internet connection.

Actions to be taken:
Install / activate Firewall if not already present in the Router. Configure firewall to allow access via ports required by the system Software chosen. Lists of essential / commonly open ports are freely available. Enforce a strong password policy for the system software / network logon.

Reasons for actions:
Attacks on commonly used ports are frequent and automated. A firewall will block / ignore pings unless the relevant port has been opened. Open Ports invite a further, more targeted attack, probably also automated. Use of strong passwords on the normal network logon increases the difficulty of getting network access. Use of strong passwords can be enforced by Software.

Constraints:
Technical: Minimal, setup and configuration tasks are simple and 'walk through' are freely available.
Financial: Minimal, a commercial quality router will almost always include a firewall.
Legal responsibilities: None as long as the data is protected by other means such as encryption.
Usability: Minimal, although enforcement of strong passwords may cause some logon errors / locked accounts.

Cost – benefit the possibility of a major system intrusion easily outweighs the minimal costs involved. The measure must be implemented.

Test No	Test description	Expected outcome	Possible further action following test
10.	Use a port scanner on the firewall.	Shows open ports.	Check use of all open ports. Close any that are not required.
11.	Set a new, weak password for network login.	Password change should be rejected.	If password is accepted, configure server security policy to require strong passwords.